Microsoft Privacy Development Standard

JC Cannon
Privacy Strategist
Corporate Privacy Group
Microsoft Corporation

Agenda

- Problem we are trying to solve
- Background of proposed solution
- How privacy development standard fits into organization
- How TCAAB can help in creation / deployment of standard

Before the Standard

- Other than Windows and Office, many product groups were building components without a privacy review
- Privacy reviews were done without regard to corporate privacy policy
- There was no consistency in how privacy reviews were performed
- No formal signoff

Purpose of the Standard

- Fulfill Microsoft's desire to build privacy-aware applications & services
- Consolidate standards and guidelines created by other product groups
- Fill void for privacy direction in product groups – once deployed

MS Privacy Development Standard
The Roadmap

MS Privacy Development Standard
Document Creation

- Derived from corporate privacy policy
- Operationalizes PD3 philosophy
- Includes privacy work from Windows, Office, MSN, and MS.com teams
- Embraces Safe Harbor Principles

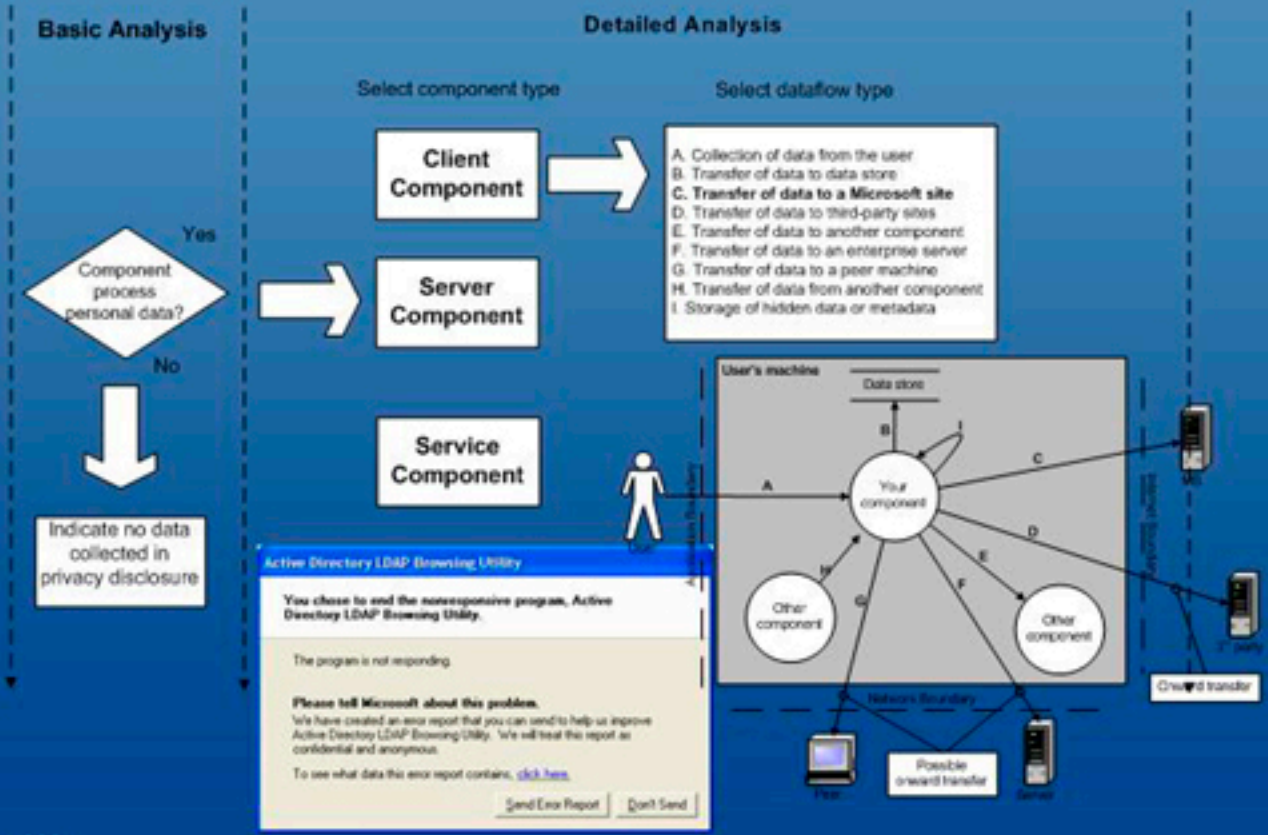
MS Privacy Development Standard
Document organization – Basic concepts

- Data classifications
  - Anonymous, PII, Sensitive PII
- Types of notice and consent
- Types of privacy controls
  - User, administrator, parental
- Data minimization
- Exception processing

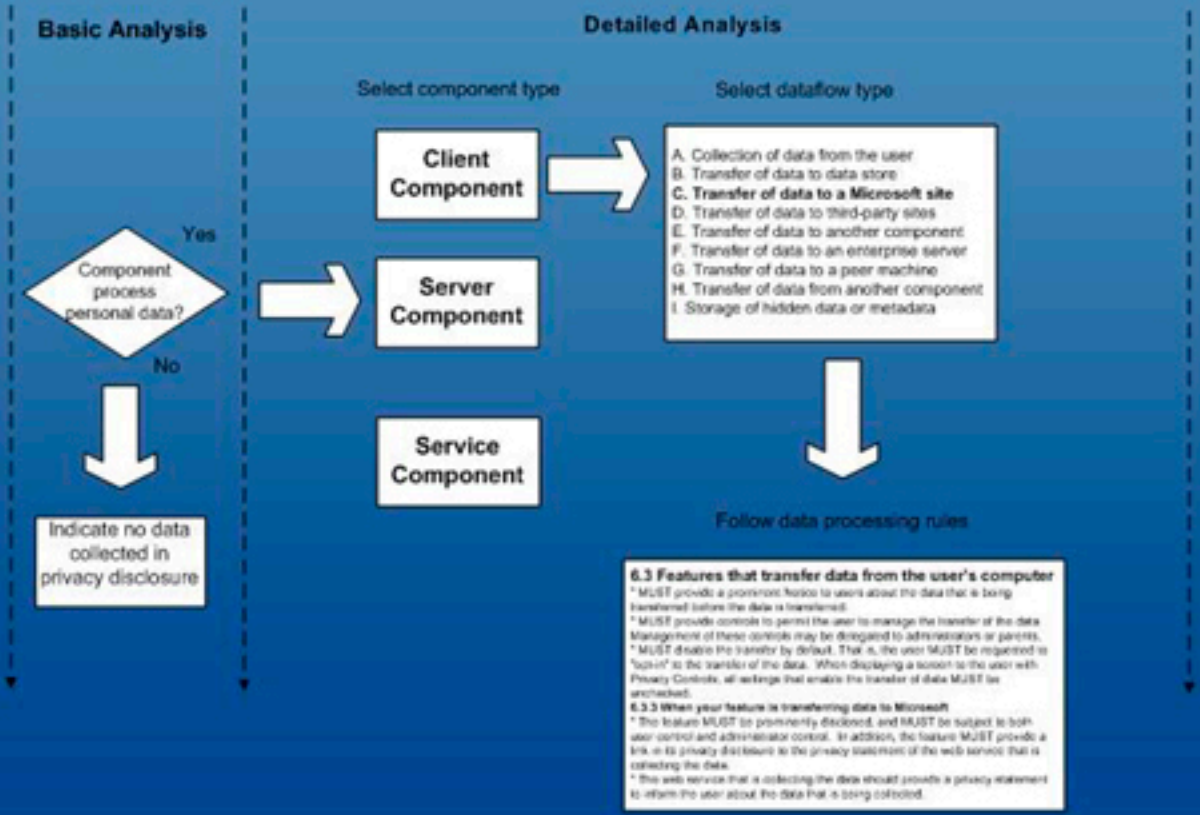
MS Privacy Development Standard
Document organization – The analysis

- Basic Privacy Analysis
  - Determine if data is being processed
  - Provide disclosure
- Detailed Analysis
  - Determine component type
    - Client, service, server
  - Select type of dataflow component uses
  - Follow rules for dataflow type

Performing an Analysis

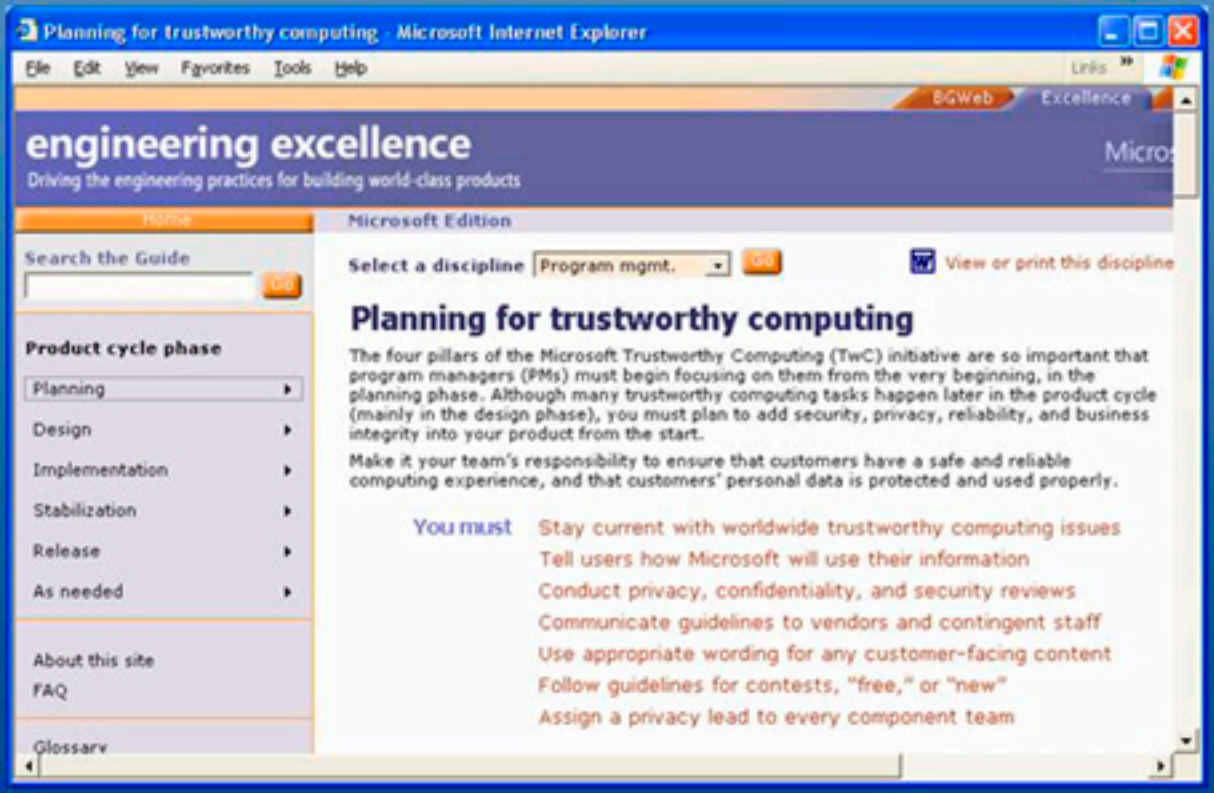


Performing an Analysis

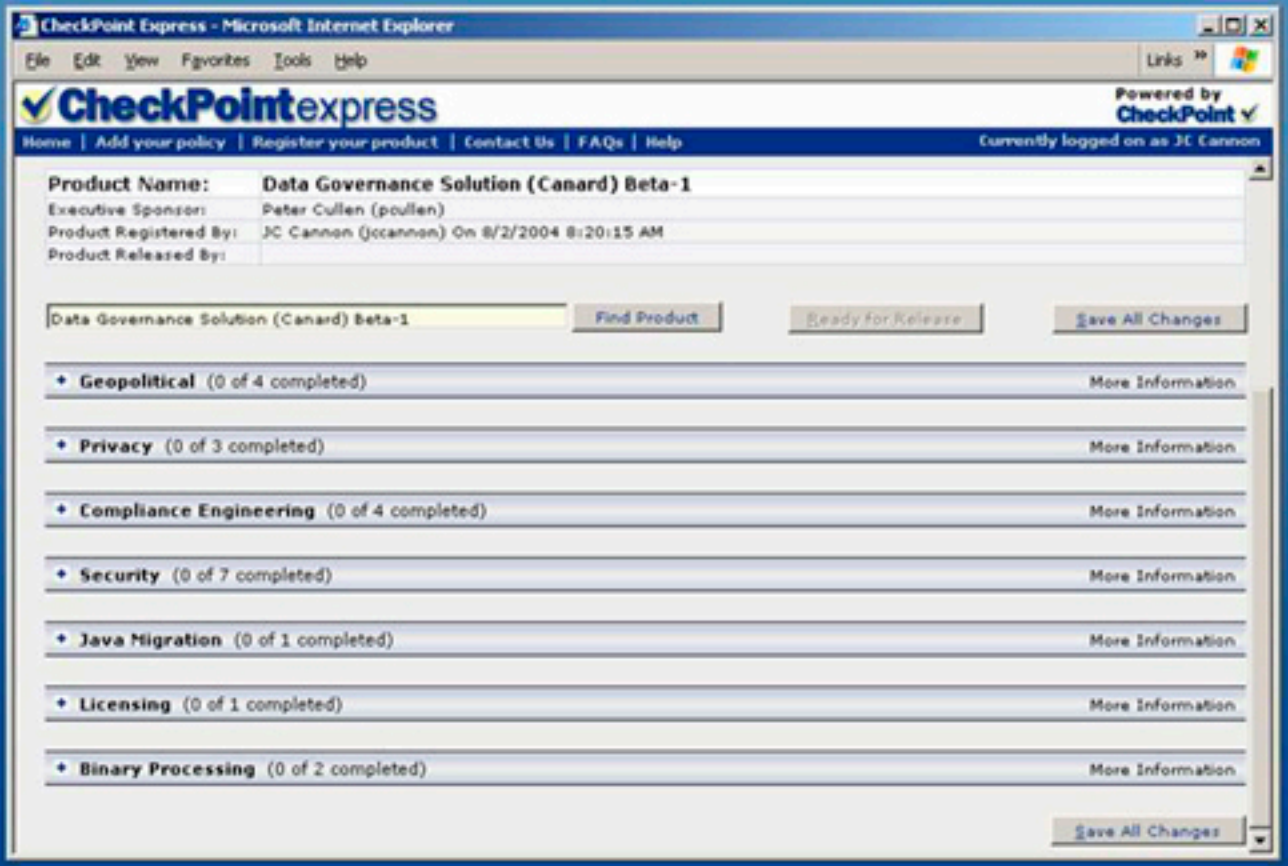


MS Privacy Development Standard
Status and Next Steps

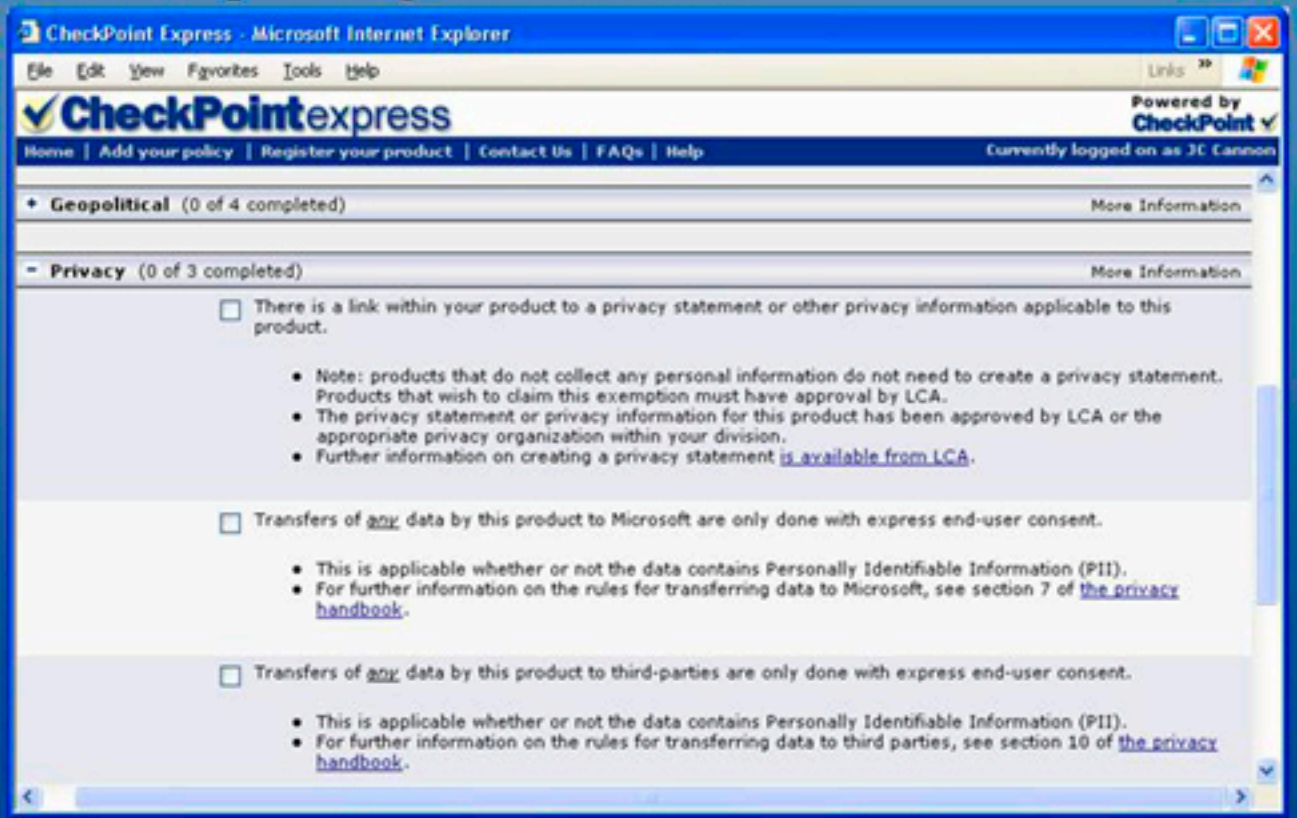
Engineering Excellence Guide



CheckPoint Express



CheckPoint Express
Privacy Requirements



Extending the Standard

Missing Elements & Challenges

- Integration with Software Dev Life Cycle
- Deployment Process
  - Standalone or integrated
- Add special topics:
  - Privacy for RFID Solutions
  - Location-based services
  - Guidelines for COPPA
  - Dealing with IP addresses
  - Best practices for advertising and configuration changes
  - Retention guidelines
  - SQM / CEIP

Feedback from TCAAB

- The best way to provide feedback is by sending a redline of the standard
- Questions to be answered:
  - IS PD3+C framework optimal?
  - How is the flow of the standard?
  - Does it cover the right topics?
  - What pieces are missing?
  - How do we adapt the standard over time?
  - Should each product group add their nuances or create their own standards?